F3

ELECTRONIC EQUIPMENT AND METHOD FOR REWRITING INSIDE PROGRAM OF THE SAME EQUIPMENT AND COMPUTER READABLE INFORMATION STORAGE MEDIUM RECORDED WITH PROGRAM HAVING FUNCTION FOR REWRITING THE SAME PROGRAM

Publication number: JP2001092668
Publication date: 2001-04-06
Inventor: SAKAMOTO KAZUYUKI
Applicant: SONY CORP
Classification:
- international: ***G06F21/22; G06F9/445; G06F15/00; G06F21/20;*** **G06F21/22; G06F9/445; G06F15/00; G06F21/20;** (IPC1-7): G06F9/445; G06F15/00
- European:
Application number: JP19990265843 19990920
Priority number(s): JP19990265843 19990920

Abstract of **JP2001092668**

PROBLEM TO BE SOLVED: To provide electronic equipment for ensuring high security related with the writing of an inside program, a method for rewriting the inside program of the electronic equipment, and a computer readable information recording medium for recording program having a function for rewriting the inside program of the electronic equipment. SOLUTION: This electronic equipment 1 capable of the rewriting of an inside program for controlling an operation is provided with a storage means 7 for storing the first identifier of a person who has authority to rewrite the inside program, identifying means 2 and 9 for identifying the second identifier of a person who tries to rewrite the inside program, and a certifying means 9 for collating thesecond identifier with the first identifier for certifying.

F3

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－92668
（P2001－92668A）
(43)公開日　平成13年４月６日(2001.4.6)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード(参考)
Ｇ０６Ｆ　9/445		Ｇ０６Ｆ　9/06	５５０Ｇ　５Ｂ０７６
9/06	５５０	15/00	３３０Ｆ　５Ｂ０８５
15/00	３３０	9/06	４２０Ｍ

審査請求　未請求　請求項の数４　ＯＬ　（全８頁）

(21)出願番号　特願平11－265843

(22)出願日　平成11年９月20日(1999.9.20)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　坂本　和之
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100096806
弁理士　岡▲崎▼　信太郎　（外１名）

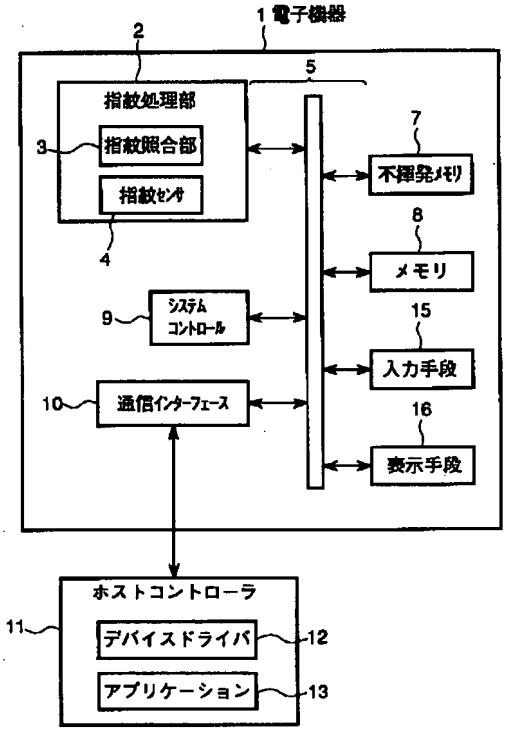
Ｆターム(参考)　5B076 BB14 FA20 FB20
5B085 AE02 AE23 AE26

(54)【発明の名称】　電子機器、電子機器の内部プログラム書き換え方法及び電子機器の内部プログラム書き換え機能を有するプログラムを記録したコンピュータ読み取り可能な情報記録媒体

(57)【要約】

【課題】　内部プログラムの書き換えに関して高いセキュリティを確保することができる電子機器、電子機器の内部プログラム書き換え方法及び電子機器の内部プログラム書き換え機能を有するプログラムを記録したコンピュータ読み取り可能な情報記録媒体を提供すること。

【解決手段】　動作を制御するための内部プログラムを書き換え可能な電子機器１であって、前記内部プログラムの書き換えについて許可されている者の第１識別子を格納する格納手段７と、前記内部プログラムを書き換えようとする者の第２識別子を識別するための識別手段２、９と、前記第２識別子を前記第１識別子と照合し、認証するための認証手段９とを設ける。



【特許請求の範囲】
【請求項１】　動作を制御するための内部プログラムを書き換え可能な電子機器であって、
前記内部プログラムの書き換えについて許可されている者の第１識別子を格納する格納手段と、
前記内部プログラムを書き換えようとする者の第２識別子を識別するための識別手段と、
前記第２識別子を前記第１識別子と照合し、認証するための認証手段とを備えることを特徴とする電子機器。
【請求項２】　前記第１識別子及び前記第２識別子は、それぞれ指紋若しくは暗号キー又はこれらの組み合わせである請求項１に記載の電子機器。
【請求項３】　動作を制御するための内部プログラムを書き換え可能な電子機器の内部プログラム書き換え方法であって、
前記内部プログラムの書き換えについて許可されている者の第１識別子を格納手段に格納する格納ステップと、
前記内部プログラムを書き換えようとする者の第２識別子を識別手段によって識別するための識別ステップと、
前記第２識別子を前記第１識別子と照合し、認証手段によって認証するための認証ステップとを有することを特徴とする電子機器の内部プログラム書き換え方法。
【請求項４】　動作を制御するための内部プログラムを書き換え可能な電子機器の内部プログラム書き換え機能を有する内部プログラムを記録したコンピュータ読み取り可能な情報記録媒体であって、
前記内部プログラムの書き換えについて許可されている者の第１識別子を格納手段に格納する格納ステップと、
前記内部プログラムを書き換えようとする者の第２識別子を識別手段によって識別するための識別ステップと、
前記第２識別子を前記第１識別子と照合し、認証手段によって認証するための認証ステップとを有する電子機器の内部プログラム書き換え機能を有するプログラムを記録したことを特徴とするコンピュータ読み取り可能な情報記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、書き換え可能な内部プログラムによって動作が制御されている電子機器、電子機器の内部プログラム書き換え方法及び電子機器の内部プログラム書き換え機能を有するプログラムを記録したコンピュータ読み取り可能な情報記録媒体に関するものである。
【０００２】
【従来の技術】近年、産業の発達によって電子機器には、様々な機能が搭載されている。この電子機器は、例えば所定のファームウェア（内部プログラム）によってその機能を発揮するように制御されている。このファームウェアは、例えば電子機器に内蔵するメモリに格納されている。このメモリは、例えばデータの書き換えが可能であり、電子機器は、このファームウェアを書き換えることによってその機能を変更することができる。従来、このファームウェアは、特定の者によってのみ書き換えられるように、例えばパスワードや電子機器のシリアル番号を入力させるといった簡易な認証手段によって認証させていた。
【０００３】
【発明が解決しようとする課題】ところが、このようなパスワードや電子機器のシリアル番号等の情報が一旦漏洩してしまうと、ファームウェアが第三者によって不正に書き換えられてしまう問題点があった。つまり、第三者が、ファームウェアの動作中（以下、「オンライン」という）にファームウェアを書き換えてしまうと、電子機器は正常な動作を行わない場合があった。
【０００４】そこで本発明は上記課題を解消し、内部プログラムの書き換えに関して高いセキュリティを確保することができる電子機器、電子機器の内部プログラム書き換え方法及び電子機器の内部プログラム書き換え機能を有するプログラムを記録したコンピュータ読み取り可能な情報記録媒体を提供することを目的としている。
【０００５】
【課題を解決するための手段】上記目的は、請求項１の発明にあっては、動作を制御するための内部プログラムを書き換え可能な電子機器であって、前記内部プログラムの書き換えについて許可されている者の第１識別子を格納する格納手段と、前記内部プログラムを書き換えようとする者の第２識別子を識別するための識別手段と、前記第２識別子を前記第１識別子と照合し、認証するための認証手段とを備えることを特徴とする電子機器により、達成される。
【０００６】上記目的は、請求項３の発明にあっては、動作を制御するための内部プログラムを書き換え可能な電子機器の内部プログラム書き換え方法であって、前記内部プログラムの書き換えについて許可されている者の第１識別子を格納手段に格納する格納ステップと、前記内部プログラムを書き換えようとする者の第２識別子を識別手段によって識別するための識別ステップと、前記第２識別子を前記第１識別子と照合し、認証手段によって認証するための認証ステップとを有することを特徴とする電子機器の内部プログラム書き換え方法により、達成される。
【０００７】上記目的は、請求項４の発明にあっては、動作を制御するための内部プログラムを書き換え可能な電子機器の内部プログラム書き換え機能を有する内部プログラムを記録したコンピュータ読み取り可能な情報記録媒体であって、前記内部プログラムの書き換えについて許可されている者の第１識別子を格納手段に格納する格納ステップと、前記内部プログラムを書き換えようとする者の第２識別子を識別手段によって識別するための識別ステップと、前記第２識別子を前記第１識別子と照

合し、認証手段によって認証するための認証ステップとを有する電子機器の内部プログラム書き換え機能を有するプログラムを記録したことを特徴とするコンピュータ読み取り可能な情報記録媒体により、達成される。

【０００８】請求項１、３又は４のいずれかの構成によれば、電子機器は、その動作を制御するための内部プログラムが書き換え可能である。この内部プログラムは、電子機器の動作を制御するためのものである。格納手段には、内部プログラムの書き換えについて許可されている者の第１識別子が格納されている。識別手段は、前記内部プログラムを書き換えようとする者の第２識別子を識別する。認証手段は、識別手段によって識別された第２識別子を格納手段の第１識別子と照合し、認証する。従って、電子機器の内部プログラムは、認証を受けた者のみが書き換えることができるようになる。このため、電子機器は、内部プログラムの書き換えに関してセキュリティを向上させることができる。

【０００９】請求項２の発明は、請求項１の構成において、前記第１識別子及び前記第２識別子は、それぞれ指紋若しくは暗号キー又はこれらの組み合わせであることを特徴とする。

【００１０】

【発明の実施の形態】以下、本発明の好適な実施の形態を添付図面に基づいて詳細に説明する。なお、以下に述べる実施の形態は、本発明の好適な具体例であるから、技術的に好ましい種々の限定が付されているが、本発明の範囲は、以下の説明において特に本発明を限定する旨の記載がない限り、これらの形態に限られるものではない。以下の説明においては、電子機器１が動作中である状態を「オンライン」という。

【００１１】図１は、本発明の第１実施形態としての電子機器１及びホストコントローラ１１の構成例を示すブロック図である。ホストコントローラ１１は、例えば作業者によって操作されるコンピュータのような電子機器であり、所定の信号線を介して電子機器１に接続されている。ホストコントローラ１１は、例えばデバイスドライバ１２及びアプリケーションプログラム１３（アプリケーション）を有する。ホストコントローラ１１は、例えば電子機器１の通信インターフェース１０との間でデータの通信制御を行う。

【００１２】デバイスドライバ１２は、例えばホストコントローラ１１の基本動作を制御するためのソフトウェアである。デバイスドライバ１２は、電子機器１のファームウェア（内部プログラム）を書き換えるための権利（以下「書き換え権」という）を電子機器１に対して要求する。ここで、「ファームウェア」とは、ハードウェアに組み込まれて動作するプログラムをいう。デバイスドライバ１２は、この書き換え権を取得すると、アプリケーション１３に対してファームウェアの書き換えコマンドの発行を許可する。尚、ホストコントローラ１４は、デバイスドライバ１２が書き換え権の取得に関与せず、アプリケーション１３が直接書き換え権の要求を行うような構成であってもよい。

【００１３】アプリケーション１３は、例えば電子機器１のファームウェアを書き換えるためのコマンドを発行するためのプログラム（電子機器の内部プログラム書き換え機能を有するプログラム）である。デバイスドライバ１２及びアプリケーション１３は、それぞれ例えば図示しないメモリに記憶されている。

【００１４】上記電子機器１は、例えば指紋処理部２（識別手段）、システムコントロール９（識別手段、認証手段）、通信インターフェース１０、バス線５、不揮発メモリ７（格納手段）、メモリ８、入力手段１５及び表示手段１６を有する。バス線５は、例えば指紋処理部２、システムコントロール９、通信インターフェース１０、不揮発メモリ７、メモリ８、入力手段１５及び表示手段１６と接続されている。この電子機器１は、指紋照合器（指紋照合器付きドア等を含む）、携帯型電話装置、情報端末、コンピュータ等の電子機器である。

【００１５】指紋処理部２は、例えば電子機器１のファームウェアを書き換えようとする作業者の識別子を識別するための処理を行う。この識別子としては、例えば指紋がある。指紋処理部２は、例えば指紋センサ４及び指紋照合部３を有する。指紋センサ４は、図２のようにＬＥＤ（Ｌｉｇｈｔ　Ｅｍｉｔｔｉｎｇ　Ｄｉｏｄｅ）２１、プリズム２０、レンズ２２及び撮像素子の一例としてのＣＣＤ（Ｃｈａｒｇｅ　Ｃｏｕｐｌｅｄ　Ｄｅｖｉｃｅ）２３を有する。ＣＣＤ２３には、指紋照合部３が接続されている。

【００１６】ＬＥＤ２１は、電子機器１のファームウェアを書き換えようとしている作業者の指Ｆが接触しているプリズム４００に対して発光する。レンズ２２は、指Ｆの指紋の凹凸情報を表す光信号を集光する。ＣＣＤ２３は、この光信号を電気信号に変換する。指紋照合部３は、この光信号を指紋画像とし、この指紋画像を図１の不揮発メモリ７に予め格納されている指紋画像と照合する。

【００１７】システムコントロール９は、例えば電子機器１全体を制御するための制御部である。システムコントロール９は、バス線５を介して接続されている指紋処理部２、通信インターフェース１０、不揮発メモリ７、メモリ８、入力手段１５及び表示手段１６を制御している。システムコントロール９は、例えばホストコントローラ１４からのファームウェア書き換え権利の要求に対して応答する。

【００１８】通信インターフェース１０は、例えばホストコントローラ１１との間でデータ通信を行うためのインターフェースである。通信インターフェース１０としては、例えばＲＳ－２３２Ｃ、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）、赤外線通信、ＬＡＮ

（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）が挙げられる。

【００１９】不揮発メモリ７は、書き換え可能な不揮発性の情報記憶媒体であり、例えば電子機器１のファームウェアの書き換え権限が付与された者の識別子、例えば指紋情報を格納している。不揮発メモリ７には、例えば指紋照合用の指紋画像データ、任意の一般データ及びファームウェア、好ましくは電子機器１のファームウェアを書き換える機能を有するプログラム（書き換えプログラム）の一部が格納されている。この書き換えプログラムの一部の機能としては、例えばホストコントローラ１４からの書き換え権要求に応答する機能である。

【００２０】不揮発メモリ７では、プログラム以外のデータはファイルという単位で分類され、１つ１つのファイルは所有者がわかる識別子を有する。そして、不揮発メモリ７には、電子機器１に対してどのような権限を有するかを上述の書き換えプログラムによって設定することができる。尚、不揮発メモリ７は、複数設けられているような構成であっても良い。この場合、各データは、複数の不揮発メモリのうち、いずれに書いてあっても良い。

【００２１】メモリ８は、例えばデータの書き換え可能な揮発性メモリであり、システムコントロール９の制御によって上述の書き換えプログラムが読み込まれ、その書き換えプログラムの作業領域として用いられる。尚、メモリ８は、複数設けられていても良い。入力手段１５は、例えば文字等を入力するためのキーボードやマウス等のポインティングデバイスである。表示手段１６は、例えば液晶ディスプレイやＣＲＴ（Ｃａｔｈｏｄｅ　Ｒａｙ　Ｔｕｂｅ）のような表示装置である。

【００２２】電子機器１は以上のような構成であり、電子機器１のファームウェアの書き換え方法について図１～図４を参照しながら説明する。図３は、図１の電子機器１のファームウェアの書き換え方法の一例を示すフローチャートである。作業者は、電子機器１のファームウェアを書き換える作業を行う者である。電子機器１は例えばオンラインであってもファームウェアを書き換えることができるので、特定の作業者のみが許可されるべきである。

【００２３】作業者は、電子機器１のファームウェアを書き換える際に、指紋センサ４に所定の指を配置させる。電子機器１は、書き換え処理を開始する（ステップＳＴ１）。電子機器１は、図１の指紋処理部２を制御して作業者の指紋画像を取り込む（ステップＳＴ２）。不揮発メモリ７には、例えば予め書き換え権限が付与された者の指紋画像に関するデータが格納されている（格納ステップ）。作業者は、例えば不揮発メモリ７に格納されたものであって表示手段１６に表示されている指紋画像から最も近いものを入力手段１５によって指定する（ステップＳＴ３）。

【００２４】電子機器１は、両者の指紋が一致しているか否かを判断する（ステップＳＴ４：識別ステップ）。一致していないと判断されると、作業者は、ファームウェアの書き換え許可に関する権限（以下、単に「書き換え権限」という）が付与されない。一方、一致していると判断されると、作業者は、さらに書き換え権限を持つ指紋か否かが判断される（ステップＳＴ５）。

【００２５】作業者は、キーボード等の入力手段１５によって予め設定されたパスワードを入力する（ステップＳＴ６）。電子機器１は、入力されたパスワードを予め設定されたパスワードと照合し、一致しているか否かを判断する（ステップＳＴ８）。一致していないと判断すると、作業者は、書き換え権限が付与されない（ステップＳＴ１７）。一方、一致していると判断されると、電子機器１は、入力されたパスワードが書き換え権限をもつ者のパスワードであるか否かを判断する（ステップＳＴ９）。

【００２６】電子機器１が書き換え権限を有する者のパスワードでないと判断すると、作業者には、書き換え権限が付与されない。一方、電子機器１が書き換え権限を有する者のパスワードであると判断すると、作業者には、書き換え権限が付与される（認証ステップ）。ホストコントローラ１１は、システムコントロール９の制御によって通信インターフェース１０を用いて、電子機器１のファームウェアを書き換える。従って、作業者は、所定の操作を電子機器１に対して行うことによって電子機器１のファームウェアを書き換えることができる。

【００２７】本発明の第１実施形態によれば、予め設定された作業者のみが電子機器１のファームウェアを書き換えることができるので、電子機器１のファームウェアの書き換えに関して従来以上にセキュリティを確保することができる。特に、電子機器１は、オンラインでファームウェアを書き換えることができる場合には、任意の者がファームウェアを書き換えることは好ましくないので、特に効果を発揮する。また、電子機器１は、ファームウェアの書き換えに関する情報が漏洩した場合であっても、ファームウェアの書き換えに際し予め設定した者の指紋等の照合が必要であるので、ファームウェアの書き換えに関してセキュリティを守ることができる。

【００２８】また、電子機器１のファームウェアの書き換え方法は、以下のようなフローチャートに従って動作しても良い。図４は、図３のフローチャートの変形例を示すフローチャートである。図４のフローチャートでは、図３のフローチャートにおいて同一の符号を付した箇所は同じ処理であるから、異なる点についてのみ説明する。尚、図４において影のついている処理（例えばステップＳＴ３、ステップＳＴ６及びステップＳＴ７）は、例えばシステムコントロール９が行っているものとする。

【００２９】図４のフローチャートでは、作業者が入力

手段１５によって入力したパスワードが、例えば不揮発メモリ７に格納されたパスワードと照合されることである。この不揮発メモリ７に格納されたパスワードは、例えば上述の書き換え権限を付与された者毎に格納されている。

【００３０】このような変形例では、上述の手法による効果に加えてさらに、指紋画像の選択等の作業者の操作をシステムコントロール９が代行することで、作業者の操作を簡素化することができる。

【００３１】第２実施形態

図５は、本発明の第２実施形態としての電子機器１及びホストコントローラ１１の構成例を示すブロック図である。図５では、第１実施形態における図１と同一の符号を付した箇所は同じ構成である。図６は、図１の電子機器１のファームウェアの書き換え方法の一例を示すフローチャートであり、図７は、図６のフローチャートの変形例を示すフローチャートである。図６及び図７では、それぞれ第１実施形態における図３及び図４と同一の符号を付した処理は同じ処理であるから、異なる点についてのみ説明する。

【００３２】第２実施形態としての電子機器１ａでは、第１実施形態としての電子機器１の構成に暗号処理部６が加えられている。暗号処理部６は、例えば公開鍵暗号法や共通鍵暗号法の暗号／復号化処理を行う。また、作業者の操作面においては、第２実施形態としての電子機器１ａでは、第１実施形態としての電子機器１において入力していたパスワードの代わりに、後述する暗号キーを入力している。

【００３３】電子機器１ａにおけるステップＳＴ１～ステップＳＴ５の処理は、第１実施形態としての電子機器１のステップＳＴ１～ステップＳＴ５の処理と同様であるので説明を省略する。ステップＳＴ５の処理が終了して、電子機器１ａは、識別された作業者の指紋を書き換え権限を有する者の指紋でないと判断すると、作業者には書き換え権限が付与されない（ステップＳＴ１７）。一方、電子機器１ａは、識別された作業者の指紋を書き換え権限を有する者の指紋であると判断すると、第１乱数を出力する（ステップＳＴ１０）。作業者は、入力手段１５によって自分の暗号キーで第１乱数を暗号化する（ステップＳＴ１１）。電子機器１ａは、暗号化された暗号文を指定された暗号キーで復号化する（ステップＳＴ１３）。電子機器１ａは、先に出力した第１乱数と、複合化された第２乱数とが一致しているか否かを判断する（ステップＳＴ１４）。

【００３４】電子機器１ａは、一致していないと判断すると作業者に書き換え権限を付与しない（ステップＳＴ１７）。一方、電子機器１ａは、一致していると判断すると暗号キーを入力した者が書き換え権限があるか否かを判断する（ステップＳＴ１５）。電子機器１ａは、書き換え権限がない者であると判断すると作業者に書き換え権限を付与しない（ステップＳＴ１７）。一方、電子機器１ａは、書き換え権限がある者であると判断すると作業者に書き換え権限を与え、第１実施形態と同様に電子機器１のファームウェアを書き換える。

【００３５】本発明の第２実施形態によれば、異なる手法であっても第１実施形態とほぼ同様の効果を発揮することができる。

【００３６】また、第２実施形態としての電子機器１ａのファームウェアの書き換え方法は、以下のようなフローチャートによって動作しても良い。図７は、図６のフローチャートの変形例を示すフローチャートである。図７のフローチャートでは、図６のフローチャートにおいて同一の符号を付した箇所は同じ処理であるから、異なる点についてのみ説明する。尚、図７において影のついている処理（例えばステップＳＴ３、ステップＳＴ１１及びステップＳＴ１２）は、例えばシステムコントロール９が行っている。図７のフローチャートでは、作業者が入力手段１５によって入力したパスワードが、例えば不揮発メモリ７に格納されたパスワードと照合されることである。この不揮発メモリ７に格納されたパスワードは、例えば上述の書き換え権限を付与された者毎に格納されている。

【００３７】このような変形例では、上述の手法による効果に加えてさらに、指紋画像の選択等の作業者の操作をシステムコントロール９が代行することで、作業者の操作を簡素化することができる。

【００３８】ところで本発明は上述した実施形態に限定されるものではない。例えば、電子機器１，１ａは、それぞれ上述の書き換え権限を有する者であるか否かを判断し認証するのに、例えば指紋照合、パスワード照合若しくは暗号照合のいずれか又はこれらいずれかの組み合わせであっても良いことはいうまでもない。

【００３９】また、上述の認証機能において認証とは、電子機器１，１ａにそれぞれ格納されたデータと、それらの外部から入力されたデータとを照合する動作を示しており、上述のような指紋照合等には限られず他の認証手段によって行われても良い。

【００４０】また、電子機器１，１ａは、例えばコンピュータや電話装置であっても良いし、上述の指紋処理部２の代わりに図８のようなカード型指紋照合部３０が設けられていても良い。

【００４１】電子機器１，１ａは、例えばドアの側等に付けたセキュリティシステムであっても良い。

【００４２】上述の電子機器１のファームウェアを書き換える機能を有するプログラムは、例えばフレキシブルディスクやＣＤ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ：商標名）等の情報記録媒体に格納されているような形態でも良い。また、この情報記録媒体としては、そのプログラムがネットワーク上に散在するコンピュータ等の電子機器に記録されたものであって、その電子機器からネットワ

ークを経由してユーザのコンピュータ等の電子機器にダウンロードされる形態のものを含んでいても構わない。

【００４３】

【発明の効果】以上説明したように、本発明によれば、内部プログラムの書き換えに関して高いセキュリティを確保することができる電子機器、電子機器の内部プログラム書き換え方法及び電子機器の内部プログラム書き換え機能を有するプログラムを記録したコンピュータ読み取り可能な情報記録媒体を提供することができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態としての電子機器及びホストコントローラの構成例を示すブロック図。

【図２】図１の指紋処理部の構成例を示すブロック図。

【図３】図１の電子機器のファームウェアの書き換え方法の一例を示すフローチャート。

【図４】図３のフローチャートの変形例を示すフローチャート。

【図５】本発明の第２実施形態としての電子機器及びホストコントローラの構成例を示すブロック図。

【図６】図５の電子機器のファームウェアの書き換え方法の一例を示すフローチャート。

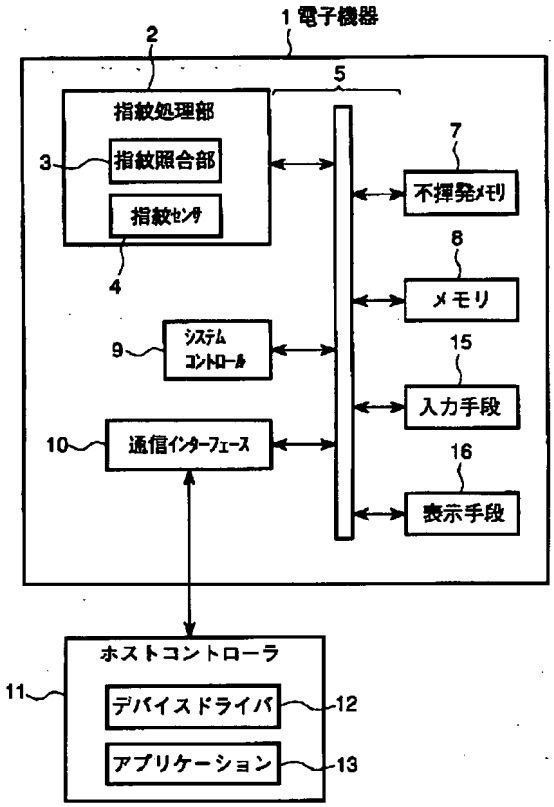
【図７】図６のフローチャートの変形例を示すフローチャート。

【図８】図２の指紋処理部の代わりに設けられたカード型指紋照合部の外観の一例を示す斜視図。

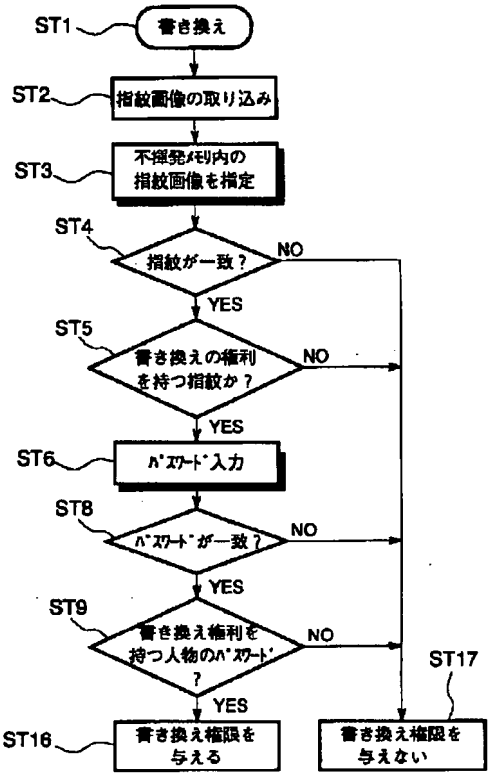
【符号の説明】

１・・・電子機器、２・・・指紋処理部（識別手段）、７・・・不揮発メモリ（格納手段）、９・・・システムコントロール（認証手段、識別手段）、１３・・・アプリケーションプログラム（電子機器の内部プログラム書き換え機能を有するプログラム）

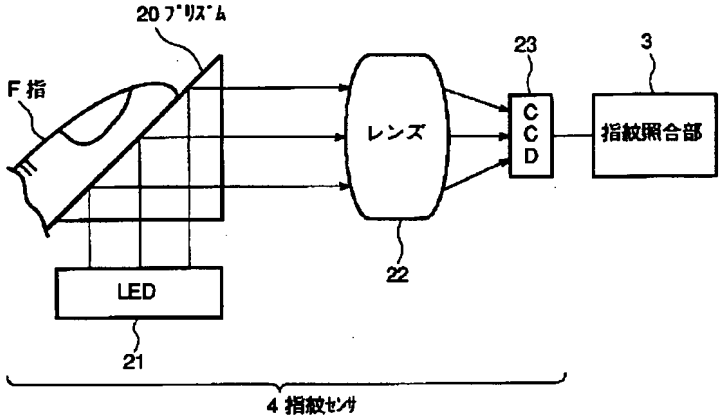
【図１】



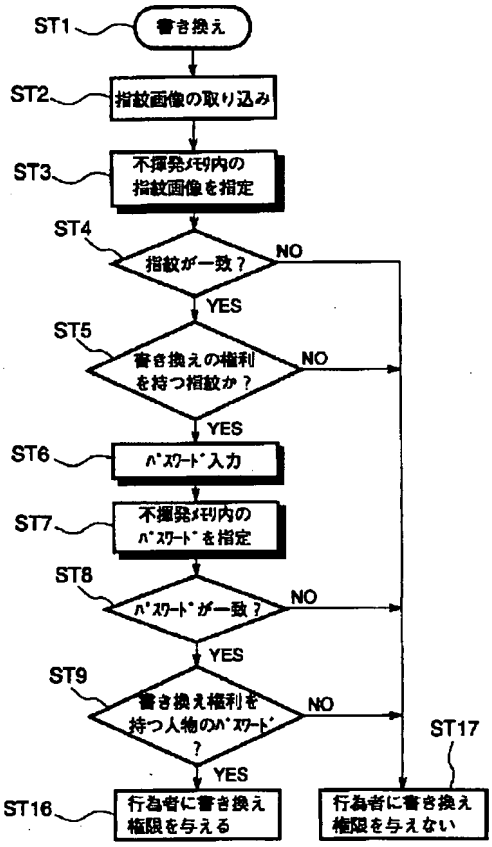
【図３】



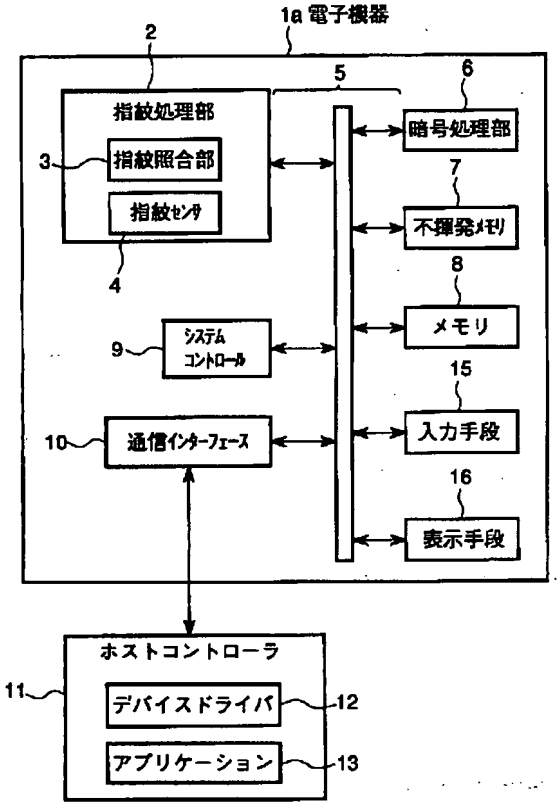
【図２】


20 ﾌﾟﾘｽﾞﾑ
F 指
レンズ
23
C
C
D
3
指紋照合部
LED
21
22
4 指紋ｾﾝｻ

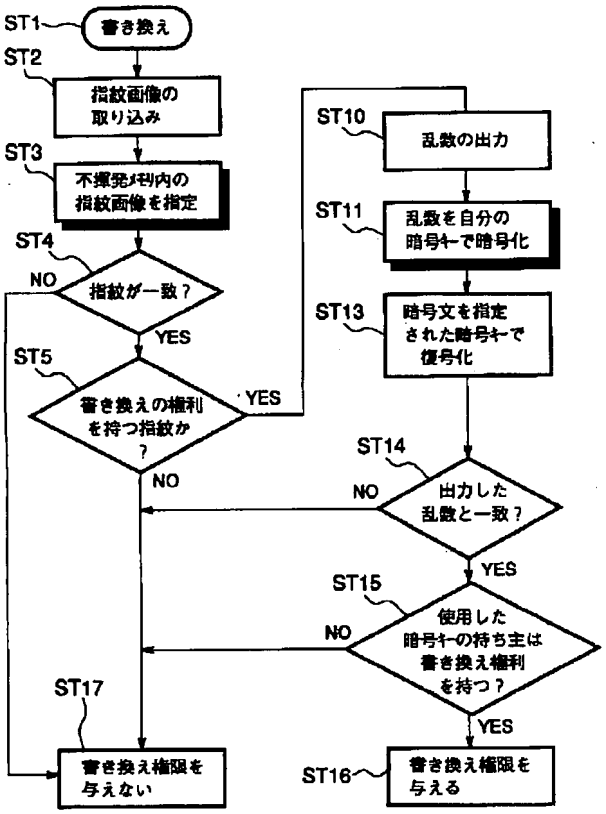
【図４】


ST1
書き換え
ST2
指紋画像の取り込み
ST3
不揮発メモリ内の
指紋画像を指定
ST4
指紋が一致？
NO
YES
ST5
書き換えの権利
を持つ指紋か？
NO
YES
ST6
ﾊﾟｽﾜｰﾄﾞ入力
ST7
不揮発メモリ内の
ﾊﾟｽﾜｰﾄﾞを指定
ST8
ﾊﾟｽﾜｰﾄﾞが一致？
NO
YES
ST9
書き換え権利を
持つ人物のﾊﾟｽﾜｰﾄﾞ
？
NO
YES
ST16
行為者に書き換え
権限を与える
ST17
行為者に書き換え
権限を与えない

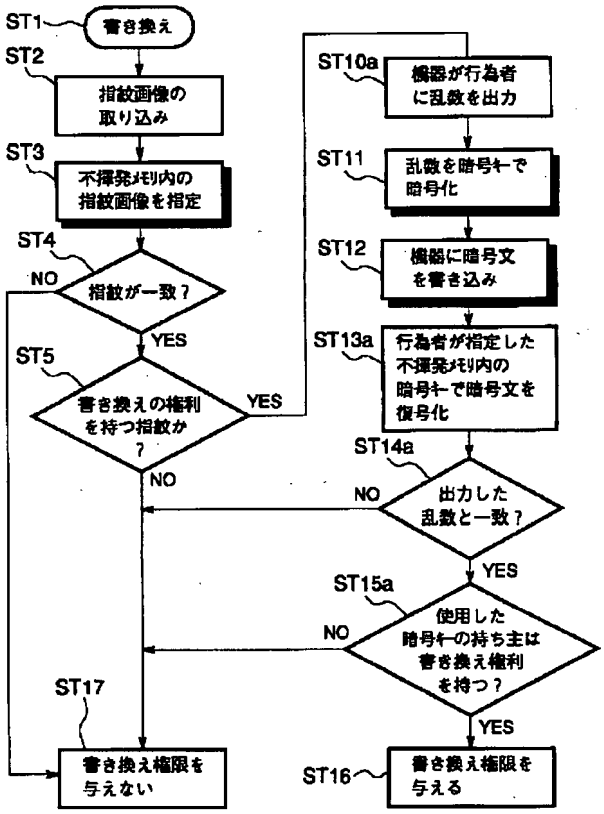
【図５】


1a 電子機器
2
5
6
指紋処理部
3
指紋照合部
指紋ｾﾝｻ
4
暗号処理部
7
不揮発メモリ
8
メモリ
9
ｼｽﾃﾑ
ｺﾝﾄﾛｰﾙ
15
入力手段
10
通信ｲﾝﾀｰﾌｪｰｽ
16
表示手段
ホストコントローラ
11
デバイスドライバ
12
アプリケーション
13

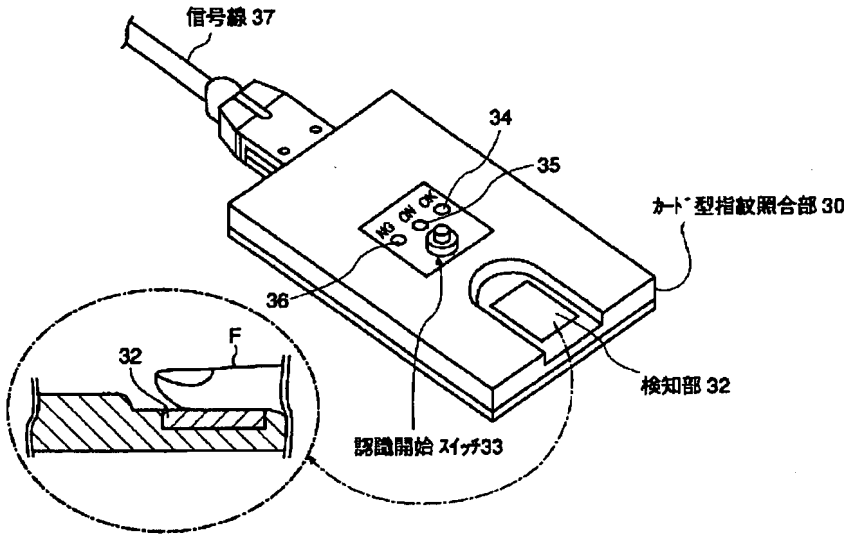
【図６】


ST1
書き換え
ST2
指紋画像の取り込み
ST3
不揮発メモリ内の指紋画像を指定
ST4
指紋が一致？
NO
YES
ST5
書き換えの権利を持つ指紋か？
YES
NO
ST10
乱数の出力
ST11
乱数を自分の暗号キーで暗号化
ST13
暗号文を指定された暗号キーで復号化
ST14
出力した乱数と一致？
NO
YES
ST15
使用した暗号キーの持ち主は書き換え権利を持つ？
NO
YES
ST16
書き換え権限を与える
ST17
書き換え権限を与えない

【図７】


ST1
書き換え
ST2
指紋画像の取り込み
ST3
不揮発メモリ内の指紋画像を指定
ST4
指紋が一致？
NO
YES
ST5
書き換えの権利を持つ指紋か？
YES
NO
ST10a
機器が行為者に乱数を出力
ST11
乱数を暗号キーで暗号化
ST12
機器に暗号文を書き込み
ST13a
行為者が指定した不揮発メモリ内の暗号キーで暗号文を復号化
ST14a
出力した乱数と一致？
NO
YES
ST15a
使用した暗号キーの持ち主は書き換え権利を持つ？
NO
YES
ST16
書き換え権限を与える
ST17
書き換え権限を与えない

【図８】


信号線 37
34
35
NG
OK
カード型指紋照合部 30
36
32
F
検知部 32
認識開始 スイッチ33